DANIEL L. WARSHAW (Bar No. 185365)
dwarshaw@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
15165 Ventura Boulevard, Suite 400
Sherman Oaks, CA 91403
Telephone: (818) 788-8300
Facsimile: (818) 788-8104

MELISSA S. WEINER (*Pro Hac Vice Forthcoming*)
mweiner@pswlaw.com
JOSEPH C. BOURNE (Bar No. 308196)
jbourne@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
800 LaSalle Avenue, Suite 2150
Minneapolis, MN 55402
Telephone: (612) 389-0600
Facsimile: (612) 389-0601

ALEXANDER L. SIMON (Bar No. 305734)
asimon@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
44 Montgomery Street, Suite 2450
San Francisco, CA 94104
Telephone: (415) 433-9000
Facsimile: (415) 433-9008

Attorneys for Plaintiff Dianne King

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA, WESTERN DIVISION

DIANNE KING, on behalf of herself and all others similarly situated,

Plaintiff,

vs.

MARRIOTT INTERNATIONAL, INC.

Defendant.

CASE NO. 2:18-cv-10173

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Dianne King ("King" or "Plaintiff") brings this class action against Defendant Marriott International, Inc. ("Marriott" or "Defendant"). Plaintiff makes the following allegations upon personal knowledge as to her own acts, and upon information and belief and the investigation of her attorneys as to all other matters, and alleges as follows:

STATEMENT OF THE CASE

1. On November 30, 2018, Marriott announced a massive customer data security breach affecting 500 million customers who stayed at Starwood-brand hotel properties between 2014 and late 2018 (hereinafter the "Data Breach").[1]

2. The Data Breach is unprecedented in its scope and duration. Approximately *500 million consumers* were affected. The database containing the stolen customer information was compromised for a period of at least *four years*—from 2014 to late 2018.

3. The Data Breach is also unprecedented in its severity and resulting safety and security implications. The database contained information on approximately 500 million consumers who made a reservation at a Starwood property, including personally identifiable information ("PII"), payment card information ("PCI"), digital copies of government-issued identification (such as driver's licenses and U.S. passports), and additional information such as arrival and departure information and dates of reservations ("Travel Information") (collectively, "Customer Data"). The compromised PII puts consumers at heightened risk of *identity theft and fraud*. The compromised PCI puts consumers at heightened risk of payment card and financial account-related *fraud losses*. And the compromised Travel Information, in addition to enhancing those other risks, also creates an

[1] Marriott International, *Starwood Guest Reservation Database Security Incident*, https://answers.kroll.com/ (last visited Dec. 3, 2018).

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

unprecedented risk of *physical intrusion or physical harm*. Put simply, the Customer Data was stolen by criminals for misuse. Marriott handed those criminals not only the information to pretend to be those consumers, or to rack up charges to their financial accounts, but also to know when they would be away from home and exactly where and when they would be.

4. For all 500 million affected consumers who were harmed by the Data Breach, the stolen Customer Data included their name and some combination of other data such as their mailing address, email address, password to the Starwood reservations system, or other information. For 327 million of those consumers, the stolen Customer Data also included some combination of their name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For an undisclosed number of those consumers, the stolen Customer Data includes payment card numbers and payment card expiration dates.[2]

5. If Marriott had simply employed reasonable, industry standard data security practices, the Data Breach would not have occurred or would have been discovered promptly.

6. Plaintiff brings this action on behalf of herself and the members of the proposed class defined below (the "Class"), seeking compensatory damages for the actual harm they have suffered and injunctive relief for the real and immediate harm they will likely suffer in the future.

THE PARTIES

Plaintiff

[2] Marriott has either been unwilling or unable to disclose how many consumers had PCI stolen.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

7. Plaintiff Dianne King is an individual and resident of Beverly Hills, California.

8. Plaintiff King and her husband jointly own four Starwood-brand timeshares, which they owned during the Class Period (defined below) and continue to own. Plaintiff King stays at Starwood-brand hotels, stayed there during the Class Period and will continue to stay there in the future. Plaintiff King has frequently used SPG points to pay for hotel stays; in those transactions she has also provided and used credit card information to pay for incidental charges.

9. Plaintiff King generally booked her hotel stays by calling the Starwood Platinum desk and occasionally booked online.

10. Plaintiff King received an email from Marriott advising her that her Customer Data was stolen in the Data Breach.

11. Plaintiff provided her Customer Data to Marriott—including by providing it to Starwood Hotels & Resorts Worldwide, LLC ("Starwood")—with the understanding that Marriott would keep her information secure, employ reasonable and adequate security measures to ensure that hackers would not compromise her Customer Data, and notify her promptly in the event of a breach.

Defendant

12. Defendant Marriott International, Inc., is a Delaware corporation with its principal place of business located at 10400 Fernwood Road, Bethesda, Maryland 20817.

13. Marriott is a leading global lodging company with more than 6,700 properties across 130 countries and territories, with reported revenues of more than $22 billion in fiscal year 2017.

14. On November 16, 2015, Marriott announced its plan to acquire Starwood. The merger closed on September 23, 2016. The transaction was for a reported $14 billion, and it made Marriott the largest hotel operator in the world.

15. Before it was acquired by Marriott, Starwood owned or operated eleven

hotel brands: W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton, and Design Hotels. Starwood also owned or operated Starwood-branded timeshare properties (collectively, the "Starwood Properties").

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) because this is a class action, there is minimal diversity, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

17. The Court has personal jurisdiction because Defendant does substantial business throughout the State of California, including this District, Defendant owns hotels or other properties in this District, and Plaintiff's claims arise out of Defendant's contacts with California and this District.

18. Venue is proper pursuant to 28 U.S.C. § 1391 because Plaintiff resides in this District, Defendant directed its business activities at residents of this District, and a substantial part of the acts and omission giving rise to Plaintiff's claims occurred in this District.

FACTUAL BACKGROUND

Marriott Collects and Promises to Safeguard Customer Data

19. Marriott collects massive amounts of Customer Data from its customers as a matter of course. According to Marriott's Privacy Statement,[3] this Customer Data includes: name; gender; postal address; telephone number; email address; credit and debit card number or other payment data; other financial information; language preference; date and place of birth; government-issued identification data,

[3] The Marriott Group, *Marriott Group Global Privacy Statement* (May 18, 2018), https://www.marriott.com/about/privacy.mi (last visited Dec. 3, 2018).

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

including but not limited to nationality, passport, or visa; important dates, such as birthdays, anniversaries, and special occasions; membership or loyalty program data; employer details; travel itinerary, tour group, or activity data; prior guest stays or interactions, goods and services purchased, and special service and amenity requests; geolocation information; and social media account ID, profile picture, and other social media data.

20. "In more limited circumstances," Marriott's Privacy Statement advises, it may also collect additional information, including: data about family members and companions, such as names and ages of children; biometric data, such as digital images; images and video and audio data collected via security cameras or body-worn cameras; and guest preferences and personalized data, such as interests, activities, hobbies, food and beverage choices, and services and amenities preferences.

21. Marriott collects this Personal Data in various ways, including: when consumers use online services (for example, when a customer makes a reservation or purchase or otherwise communicates with Marriott); when consumers use customer care centers (via phone, email, or online chat); through owners and franchisees; from authorized licensees; from strategic business partners; by collecting it from other sources, such as public databases, joint marketing partners, and other third parties; and by collecting it from internet-connected devices and physical and mobile location-based services.

22. Marriott recognizes its obligation to safeguard Customer Data, and consumers' reasonable expectation that it will do so. For instance, Marriott's Privacy Statement claims that "we respect your privacy."

23. Marriott's Privacy Statement indicates that it will use Customer Data only in certain, limited ways: to provide the services requested by consumers; to personalize services according to consumers' personal preferences; to communicate with consumers about goods and services according to their personal preferences; to

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

manage consumers' participation in its loyalty program; to offer participating in sweepstakes, activities, events, and promotions; and for business purposes such as "data analysis, audits, security and fraud monitoring and prevention."

24. Marriott's Privacy Statement indicates that it will disclose Customer Data only to a limited set of specific, authorized third parties. These include other companies within the Marriott Group, owners and franchisees, strategic business partners, and service providers.

25. Marriott's Privacy Statement promises "to use reasonable organizational, technical and administrative measures to protect Personal Data."

26. Marriott's Privacy Statement incorporates by reference its Privacy Shield Guest Privacy Policy.[4] The Privacy Shield Guest Privacy Policy is largely consistent with the Privacy Statement. It also reiterates and expands upon Marriott's promise to safeguard Customer Data: "We use reasonable physical, electronic, and administrative safeguards to protect your Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the nature of the Personal Data and the risks involved in processing that information."

27. Marriott is correct to recognize that its customers place high value on data security and privacy. Plaintiff and the Class members would not have stayed at the Starwood Properties, used their payment cards, or otherwise provided their Customer Data to Marriott if they had known that Marriott did not take reasonable and necessary steps to safeguard their Customer Data.

An Unauthorized Third Party Stole the Customer Data

28. The Data Breach affects approximately 500 million consumers who made reservations at Starwood Properties between 2014 and late 2018.

[4] Marriott International, Inc., *Marriott U.S. Privacy Shield Guest Privacy Policy* (May 18, 2018), https://www.marriott.com/about/global-privacy.mi (last visited Dec. 3, 2018).

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

29. All 500 million affected consumers had some Customer Data stolen, including their name and some combination of other data such as their mailing address, email address, or other information.

30. For 327 million consumers, the stolen Customer Data also included some combination of their name, mailing address, phone number, email address, passport number, SPG account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences.

31. For an undisclosed number of consumers, the stolen Customer Data includes payment card numbers and payment card expiration dates.

Marriott Did Not Discover the Data Breach for Four Years

32. According to Marriott, the Data Breach began no later than an unspecified time in 2014.

33. On September 8, 2018, Marriott received an alert from an internal security tool that there was an attempt to access the Starwood guest reservation database (the "Database").

34. Marriott claims that the last unauthorized access that was part of the Data Breach occurred on or before September 10, 2018.

35. During the course of its investigation, Marriott discovered that there was unauthorized access to the Starwood network dating back to 2014. Marriott also learned that an unauthorized party had copied and encrypted information, and that the unauthorized party took steps toward removing it from the Starwood network. On November 19, 2018, Marriott decrypted the information and determined that the contents were from the Database.

Marriott Failed to Use Reasonable Data Security Practices

36. If Marriott had used reasonable data security practices, the Data Breach would not have occurred, or if it had occurred, its duration and scope would have been far less severe.

37. For example, if Marriott used an intrusion detection and prevention

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

platform to protect the Customer Data, this breach could have been avoided. Suspicious activity could have been identified and intrusion prevented. Furthermore, the significant length of time between the breach and discovery suggest that Marriott failed to employ routine pattern analyses to troll for data breaches.

38. Furthermore, given the sensitive nature of the data Marriott collected, it should have had in place a robust data loss prevention platform, which if properly monitored could have safeguarded this data. Marriott admits in its statement that an external unauthorized party was able to move and then encrypt sensitive customer data in preparation for egress from the Marriott network.

39. If Marriott did employ an intrusion detection and prevention platform and a data loss prevention platform, they were not properly configured or managed.

40. A data loss prevention tool is an industry standard practice for protecting sensitive data—which applies, at minimum, to PCI, passports, and travel patterns and bookings. Because Marriott maintained the Customer Data in a single Database, it needed to treat *all* of the Customer Data as sensitive.

41. A data loss prevention tool should have preemptively identified the movement of the sensitive data within the Database before it was extracted.

42. Even if Marriott did not use a data loss prevention tool, the sheer duration of the Data Breach proves that Marriott failed to employ reasonable and competent data security practices.

43. Technology security company FireEye has a metric called "breach to discovery." This measures the median time between when a data security breach first occurs and when it is detected. The median breach to discovery time period has shrunk in recent years from over 365 to under 100 days.

44. The fact that it took Marriott *four years* or more to detect the Data Breach, when the median discovery period is *under 100 days*, demonstrates that Marriott failed to employ reasonable, industry standard data security practices to safeguard the Customer Data.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

45. It is inconceivable that it would have taken four years to discover the Data Breach if Marriott had, for example, employed a "Hunter team," which would proactively and iteratively search through networks to detect and isolate advanced threats. Use of a hunter team is appropriate when protecting sensitive data on a large scale, as Marriott did—or was supposed to.

The Customer Data Is Valuable to Criminals

46. PII data is highly coveted and a frequent target of hackers. PII data may be less protected and regulated than other data, such as PCI, and so it is often easily taken.

47. PII is frequently sought by criminals. For instance, in the widely publicized Target data breach, in addition to stealing PCI relating to 40,000 payment cards, hackers also stole PII pertaining to 70,000 customers.

48. Biographical data is also highly sought by data thieves. Biographical data gained from multiple sources is increasingly used to perpetrate more and larger thefts. For example, "synthetic identity theft" occurs when thieves create new identities by combining real and fake identifying information, and then using those identities to open new accounts. Synthetic identity theft is harder to unravel than traditional identity theft.

49. PCI is heavily regulated. The Payment Card Industry Data Security Standard ("PCI DSS") is a set of requirements designed to ensure that companies maintain consumer payment card information in a secure environment. It is a basic requirement of PCI DSS to protect stored cardholder data.

50. PII and PCI are more valuable when they are taken together.

51. Illicitly obtained PII and PCI are sold on the black market as products at a set price.

52. Because of the value of PII and PCI, there have been numerous data breaches in the hospitality industry in recent years, including several hotel chains. Following the Wyndham data breach, the Federal Trade Commission even brought

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

an action against Wyndham based on its failure to provide reasonable protection for customer data. As a result, Marriott either knew or should have known of the importance of safeguarding the Customer Data. But despite that knowledge, Marriott opted to maintain an insufficient and inadequate system to protect the Customer Data.

The Data Breach Will Result in Identity Theft and Fraud

53. The Customer Data was stolen for a reason: it is valuable in the hands of those who will misuse it. It allows criminals to commit identity theft and fraud, which will continue to occur using the Customer Data.

54. Identity theft occurs when someone uses another person's PII to commit fraud or other crimes. As many as 10 million people in the United States have their data stolen every year. Once identity thieves have personal information like the Customer Data that was stolen in this case, they can drain bank accounts, run up or open new credit cards, open new utility accounts, get medical treatment on your health insurance, or submit fraudulent tax returns to obtain tax refunds.

55. Identity thieves can commit various types of government fraud, including immigration fraud, obtaining a driver's license in the victim's name but with another's picture, obtain government benefits, or file a fraudulent tax return to obtain a fraudulent refund.

56. Some of this activity may not become known for years. Indeed, in some instances, it may not occur for years. That is particularly true when, as here, protection services are provided to victims for a fixed period, such as the one year that Marriott has offered to provide Web Watcher services to its affected customers.

57. Once identity theft is detected, fixing it is not easy. It takes many victims months to resolve the problems caused by identity theft. It takes some up to a year.

The Data Breach Is Dangerous to Plaintiff and Class Members

58. The Marriott Data Breach is not a "typical" data breach. It did not

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

involve only PII and PCI, although that is bad enough. Instead, it also contained Travel Information, such as arrival and departure information and dates of reservations.

59. With this sensitive Travel Information, a criminal who wishes to target a particular individual could use pinpointed travel information such as the location of upcoming hotel reservations, down to the city and particular dates of travel—including even expected time of arrival and departure.

60. If this criminal wished to rob the person's home, it would be much easier, knowing that they were not home and would not be returning.

61. Further, and even more terrifying, if this criminal instead wished to physically attack a person, it would be easier knowing where they would be, particularly dates away from home.

62. These risks associated with the Travel Information gave Marriott all the more reason to take the necessary steps to safeguard the Travel Information and the rest of the Customer Information that it stored together in a single Database. Marriott, however, did not.

Plaintiff and the Class Members Suffered Damages

63. Marriott's failure to properly safeguard Plaintiff and Class members' Customer Data directly and proximately caused the Data Breach.

64. As a direct and proximate result of Marriott's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud and threat to their personal safety. Plaintiff and Class members must take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

65. Plaintiff and the Class members have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft caused by their passport, payment card, and personal information being placed in the hands of criminals;

c. the improper disclosure of their private information;

d. loss of privacy;

e. ascertainable losses in the form of out-of-pocket expenses and the value of the time reasonably incurred to remedy or mitigate the effects of the Data Breach;

f. ascertainable losses in the form of deprivation of the value of their PII and PCI, for which there is an established national and international market;

g. overpayments to Marriott for products and services purchased, in that a portion of the price paid for such products and services was for the costs of reasonable and adequate safeguards and security measures to protect their Customer Data—which Marriott did not provide; and

h. the loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were able to obtain from their accounts.

66. While Plaintiff and the Class members' Customer Data has been stolen, the same (or a copy of the same) Customer Data continues to be held by Marriott. Plaintiff and the Class members have an interest in ensuring that this information is

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

secured and remains secured and will not be subject to further theft.

CLASS ACTION ALLEGATIONS

67. Pursuant to Rule 23(b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure, Plaintiff brings this lawsuit on behalf of herself and on behalf of the proposed nationwide class (the "Class") defined as follows:

> All persons residing in the United States whose Customer Data was disclosed in the Data Breach during the Class Period.

68. Maryland law should apply extraterritorially in this case because Defendant is headquartered in Maryland; the decisions, actions, and inactions causing in the Data Breach occurred in Maryland; and Maryland has the greatest interest in regulating Defendant's conduct.

69. If, however, the Court declines to apply Maryland law nationwide, then Plaintiff seeks—in the alternative—certification of a proposed California subclass (the "California Subclass") pursuant to Rule 23(b)(2), (b)(3), and (c)(4), defined as follows:

> All persons residing in California whose Customer Data was disclosed in the Data Breach during the Class Period.

70. Excluded from the Class are Defendant and any entities in which Defendant or its subsidiaries or affiliates have a controlling interest; Defendant's officers, agents, and employees; and all persons who make a timely election to be excluded from the Class. Also excluded from the Class are the judges and court personnel in this action and any members of their immediate family.

71. The "Class Period" is defined as the period during which the Data Breach occurred, from 2014 through September 10, 2018. Plaintiff reserves the right to redefine the Class Period if discovery shows that the Data Breach occurred for a longer or different period of time than Defendant has so far disclosed.

72. **Numerosity:** The members of the Class are so numerous that joinder of

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

all Class members would be impracticable. Plaintiff reasonably believes that Class members number in the millions or hundreds of millions of people. Defendant has acknowledged that the information of approximately 500 million customers was compromised in the Data Breach. The names and addresses of the Class members are identifiable through documents Defendant maintains.

73. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

a. Whether Defendant owed a legal duty to Plaintiff and Class members to exercise due care in collecting, storing, and safeguarding their Customer Data;

b. Whether Defendant breached a legal duty to Plaintiff and Class members to exercise due care in collecting, storing, and safeguarding their Customer Data;

c. Whether Defendant had an implied contractual obligation to use reasonable security measures in safeguarding the Customer Data;

d. Whether Defendant breached its implied contractual obligation to use reasonable security measures in safeguarding the Customer Data;

e. What security measures Defendant must use to comply with its implied contractual obligation and legal duty to safeguard Customer Data;

f. Whether Defendant knew or should have known of the susceptibility of its computer systems to a data breach;

g. Whether Defendant's security measures to protect its computer systems were reasonable in light of industry data security standards and recommendations;

h. Whether Defendant willfully, recklessly, or negligently failed to

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class members' Customer Data;

i. Whether Plaintiff's and Class members' Customer Data was accessed, exposed, compromised, or stolen in the Data Breach;

j. Whether Defendant was negligent in failing to implement reasonable and adequate security procedures and practices;

k. Whether Defendant's failure to implement adequate data security measures allowed the breach of its computer systems to occur;

l. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Plaintiff's and Class members' Customer Data;

m. Whether Defendant's conduct constituted deceptive trade practices;

n. Whether Defendant's conduct violated the Maryland Consumer Protection Act;

o. Whether Defendant's conduct violated the Maryland Personal Information Protection Act;

p. Whether Defendant's conduct violated the California Customer Records Act;

q. Whether Defendant's conduct violated the California Unfair Competition Law;

r. Whether Plaintiff and Class members are entitled to equitable relief, including, but not limited to, injunctive relief; and

s. Whether Plaintiff and Class members are entitled to damages or other monetary relief, and the amount thereof.

74. Defendant engaged in a common course of conduct giving rise to the

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

the legal rights sought to be enforced by Plaintiff individually and on behalf of the Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

75. **Typicality:** Plaintiff's claims are typical of Class members' claims because, among other things, Plaintiff and Class members were injured through Defendant's substantially uniform misconduct. Plaintiff is advancing the same claims and legal theories on behalf of themselves and Class members, and there are no defenses that are unique to Plaintiff's claims. Plaintiff's and Class members' claims arise from the same operative facts and are based on the same legal theories.

76. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class members she seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation, including data privacy and data security practices litigation; and Plaintiff will prosecute this action vigorously for the benefits of the Class. Class members' interests will be fairly and adequately protected by Plaintiff and their counsel.

77. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and Class members is relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

78. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

79. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to, whether Defendant utilized reasonable data security practice and whether Defendant is liable for its misconduct.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

Negligence

80. Plaintiff incorporates and realleges, as though fully set forth herein, each and every allegation set forth the in the preceding paragraphs of this Complaint.

81. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Customer Data in its possession form being compromised, lost, stolen, accessed, and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Defendant's security system to ensure that Plaintiff's and the Class's Customer Data in Defendant's possession was adequately secured and protected. Defendant further owed a duty to Plaintiff and the Class to implement processes that would detect a breach of its security system in a timely

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

manner and to timely act upon warnings and alerts, including those generated by its own security systems.

82. Defendant owed a duty to Plaintiff and the Class to provide security, consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the Customer Data of Plaintiff and the Class.

83. Defendant owed a duty of care to Plaintiff and the Class because they were foreseeable and probable victims of any inadequate security practices. Defendant solicited, gathered, and stored the Customer Data of Plaintiff and the Class to use that information for its own business purposes. Defendant knew it inadequately safeguarded such information on its computer systems and that hackers routinely attempt to access this valuable data without authorization. Defendant had prior notice that its systems were inadequate by virtue of the earlier breaches that preceded this one, but it continued to maintain those inadequate systems to the ultimate detriment of its customers like Plaintiff and the Class. Defendant knew or should have known that a breach of its systems would cause damages to Plaintiff and the Class and Defendant had a duty to adequately protect such sensitive personal and financial information.

84. Defendant owed a duty to timely and accurately disclose to Plaintiff and the Class that their personal and financial information had been or was reasonably believed to have been compromised. Timely disclosure was required, appropriate, and necessary so that, among other things, Plaintiff and the Class could take appropriate measures to avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credits reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Defendant's misconduct.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

85. Defendant knew, or should have known, the risks inherent in collecting and storing the Customer Data of Plaintiff and the Class, and of the critical importance of providing adequate security of that information.

86. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff the Class. Defendant's misconduct included, but was not limited to, its failure to take steps and opportunities to prevent and stop the data breach as set forth herein.

87. Defendant breached the duties it owed to Plaintiff and the Class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the personal and financial information of Plaintiff and the Class.

88. Defendant breached the duties it owed to Plaintiff and the Class by failing to properly implement technical systems and security practices that could have prevented the loss of the Customer Data.

89. Defendant breached its duties to Plaintiff and the Class to timely and accurately disclose that Plaintiff's and the Class's Customer Data in Defendant's possession had been or was reasonably believed to have been stolen or compromised.

90. Defendant's failure to comply with its legal obligations by causing delay between the date of intrusion and the date Defendant disclosed the data breach further evidences Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class's Customer Data in Defendant's possession.

91. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their Customer Data would not have been compromised.

92. The injury and harm suffered by Plaintiff and the Class, as set forth above, was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class's Customer

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

Data within Defendant's possession. Defendant knew or should have known that its systems and technologies for processing, securing, safeguarding, and deleting Plaintiff's and the Class's Customer Data were inadequate and vulnerable to being breached by hackers.

93. Plaintiff and the Class suffered injuries and losses described herein as a direct and proximate result of Defendant's conduct resulting in the data breach, including Defendant's lack of adequate and reasonable security measures. Had Defendant implemented such adequate and reasonable security measures, Plaintiff and the Class would not have suffered the injuries alleged, as the Data Breach would likely have not occurred.

94. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class have suffered injury and are entitled to damages in the amount to be proven at trial.

SECOND CLAIM FOR RELIEF

Breach of Implied Contract

95. Plaintiff incorporates and realleges, as though fully set forth herein, each and every allegation set forth the in the preceding paragraphs of this Complaint.

96. Defendant represented to Plaintiff and the Class, in its Privacy Statement and Privacy Policy, that it would use reasonable and adequate measures to protect their Customer Data and to safeguard their privacy.

97. Plaintiff and the Class shared personal information with Defendant, such as dates of birth, passport numbers, credit and debit cards numbers and other payment data, employer details, geolocation information, and other personal and confidential information as described herein.

98. Plaintiff and the Class performed their part of the contract. They stayed at Starwood Properties or otherwise used Defendant's goods and services. And they

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

allowed and continued to allow Defendant to store, maintain, and safeguard their personal and confidential information.

99. When Plaintiff and the Class provided their personal and confidential information to Defendant, they entered into implied contracts with the Defendant, pursuant to which Defendant agreed to protect their information, and to timely and accurately notify Plaintiff and the Class if their data had been breached or compromised, in accordance with Defendant's promises in its Privacy Statement and Privacy Policy.

100. Plaintiff and the Class would not have provided and entrusted their personal and confidential information to Defendant in the absence of the implied contract between them.

101. Plaintiff and the Class fully performed their obligation under the implied contracts with Defendant.

102. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect the personal and confidential information of Plaintiff and the Class and by failing to provide timely and accurate notice to them that their information was compromised in and as a result of the Data Breach.

103. As a direct and proximate result of Defendant's breaches of the implied contract between Defendant and Plaintiff and the Class, Plaintiff and the Class sustained actual losses and damages as described herein.

THIRD CLAIM FOR RELIEF

Maryland Personal Information Protection Act

Md. Comm. Code §§ 14-3501, et seq.

104. Plaintiff incorporates and realleges, as though fully set forth herein, each and every allegation set for the in the preceding paragraphs of this Complaint.

105. Md. Comm. Code § 14-3503(a) provides that "[t]o protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations."

106. Defendant is a business as defined under Md. Comm. Code §§ 14-3501(b)(1) and (2).

107. Plaintiff and the Class are "customers" as defined under Md. Comm. Code §§ 14-3502(a).

108. Plaintiff's and the Class's Customer Data , as alleged herein, includes "Personal Information" as defined under Md. Comm. Code § 14-3501(e)(1).

109. Defendant violated Md. Comm. Code § 14-3503 by failing "to maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations."

110. The Data Breach, as alleged herein, was a "breach of the security of a system" as defined by Md. Comm. Code § 14-3504(a)(1).

111. Md. Comm. Code § 14-3504(b)(1) provides that "[a] business that owns or licenses computerized data that includes personal information of an individual residing in the State, when it discovers or is notified of a breach of the security of a system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach."

112. Md. Comm. Code §§ 14-3504(b)(2), (b)(3), (c)(2), and (c)(3) provides that "[i]f, after the investigation is concluded, the business determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused, the business shall notify the individual of the breach" and "the notification shall be given as soon as reasonably practicable."

113. After Defendant discovered the Data Breach, Defendant was required to disclose the Data Breach in a timely and accurate manner under Md. Comm.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

Code §§ 14-3504(b)(2), (b)(3), (c)(2), and (c)(3).

114. Defendant violated Md. Comm. Code §§ 14-3504(b)(2), (b)(3), (c)(2), and (c)(3) by failing to disclose the Data Breach in a timely and accurate manner.

115. As a direct and proximate result of Defendant's violation of Md. Comm. Code §§ 14-3504(b)(2), (b)(3), (c)(2), and (c)(3), Plaintiff and the Class suffered damages as alleged herein.

116. Pursuant to Md. Comm. Code § 14-3508, Defendant's violation of Md. Comm. Code §§ 14-3504(b)(2), (b)(3), (c)(2), and (c)(3) are an unfair or deceptive trade practices under the Maryland Consumer Protection Act, Md. Comm. Code §§ 13-101, *et seq.* and subject to the enforcement and penalty provisions contained in the Maryland Consumer Protection Act.

117. Plaintiff and the Class seek relief under Md. Comm. Code §13-408, including actual damages and attorney's fees.

FOURTH CLAIM FOR RELIEF

Maryland Consumer Protection Act

Md. Comm. Code §§ 13-301, et seq.

118. Plaintiff incorporates and realleges, as though fully set forth herein, each and every allegation set for the in the preceding paragraphs of this Complaint.

119. Defendant is a "person" as defined by Md. Comm. Code. § 13-101(h).

120. Defendant's conduct as alleged herein related to "sales", "offers for sale" or "bailment" as defined by Md. Comm. Code. § 13-101(i) and § 13-303.

121. Plaintiff and the Class are "consumers" as defined by Md. Comm. Code. § 13-101(c).

122. Defendant advertised, offered, or sold "consumer goods" or "consumer services" as defined by Md. Comm. Code § 13-101(d).

123. Defendant advertised, offered, or sold "consumer goods" or "consumer services" in the State of Maryland and engaged in trade or commerce directly or or indirectly affecting the people of Maryland.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

124. Defendant violated Md. Comm. Code § 13-301 by engaging in unfair and deceptive trade practices, including:

a. False or misleading oral or written statements that have the capacity, tendency, or effect of deceiving or misleading consumers;

b. Failing to state a material fact where the failure deceives or tends to deceive;

c. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;

d. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

125. Defendant violated Md. Comm. Code § 13-303 by engaging in unfair and deceptive trade practices in connection with the offer for sale or sale of consumer goods or consumer services or services with respect to the extension of consumer credit, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members' Customer Data , which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class's personal and confidential information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3501, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class member's personal and confidential information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class's information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3501;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class's information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class's information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3501.

126. Defendant's representations and omission were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal and

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

confidential information. Defendant's misrepresentations and omission would have been important to a significant number of consumers making financial decisions.

127. Defendant intended to mislead Plaintiff and the Class and induce them to rely on its misrepresentations and omissions.

128. Had Defendant disclosed to Plaintiff and the Class that its data systems were not secure and vulnerable to attack, Defendant would have been forced to adopt reasonable security measures and comply with the law.

129. Defendant acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiff's and the Class's rights. Defendant was on notice of the possibility of the Data Breach due to well-publicized data breaches occurring previously, including in the hospitality industry.

130. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and the Class have suffered and will continue to suffer injury, including ascertainable losses of property, monetary and non-monetary damages, including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, and increased, imminent risk of fraud and identity theft' and loss of value of their Customer Data .

131. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

FIFTH CLAIM FOR RELIEF

Violation of California Customer Records Act

Cal. Civ. Code §§ 1798.80, *et seq.*

(On behalf of the California Subclass, in the alternative)

132. Plaintiff incorporates and realleges, as though fully set forth herein, each and every allegation set forth the in the preceding paragraphs of this Complaint.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

133. California Civil Code § 1798.81.5 clearly and expressly states the intent of the legislature: "It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

134. Further, California Civil Code § 1798.81.5(b) requires any "business that owns, licenses, or maintains personal information about a California resident [to] implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

135. Defendant owns, maintains, and licenses personal information, within the meaning of § 1798.81.5, concerning Plaintiff and the Class.

136. Defendant violated Civil Code § 1798.81.5 by failing to implement reasonable measures to protect the personal information of Plaintiff and the Class.

137. The data breach described above occurred as a direct and proximate result of Defendant's violations of Section 1798.81.5 of the California Civil Code.

138. California Civil Code § 1798.82(a) provides: "A person or business that conduct business in California, and that owns or licenses computerized data that include personal information, shall disclose a breach of the security system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay . . . ."

139. California Civil Code § 1798.82(b) provides that "[a] person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security data immediately following discovery, if

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

140. Defendant is a business that owns or licenses computerized data that includes personal information as defined by California Civil Code §§ 1798.80, *et seq.*

141. In the alternative, Defendant maintains computerized data that includes personal information that it does not own as defined by California Civil Code §§ 1798.80, *et seq.*

142. Plaintiff and the California Subclass members' Customer Data (including but not limited to their names, email addresses, payment card numbers, and driver's license or passport numbers) includes personal information covered by California Civil Code § 1798.81.5(d)(1).

143. Because Defendant reasonably believed that the personal information of Plaintiff and the Class was acquired by unauthorized persons, it had an obligation to disclose the data breach described above in a timely and accurate fashion under California Civil Code California Civil Code § 1798.82(a), or in the alternative, under California Civil Code California Civil Code § 1798.82(b).

144. Thus, by failing to disclose the data breach in a timely and accurate manner, Defendant violated California Civil Code § 1798.82.

SIXTH CLAIM FOR RELIEF

Violation of Unfair Competition Law

Cal. Bus. & Prof. Code §§ 17200, et seq.

(On behalf of the California Subclass, in the alternative)

145. Plaintiff incorporates and realleges, as though fully set forth herein, each and every allegation set forth in the preceding paragraphs of this Complaint.

146. Defendant has engaged in unfair competition within the meaning of California Business and Professions Code §§ 17200, *et seq.* (the "UCL") because Defendant's conduct is unfair and unlawful as herein alleged. Plaintiff and the Class

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

were injured by Defendant's conduct because Defendant failed to properly maintain Plaintiff's and the Class's Customer Data and unreasonably delated in informing the public, including Plaintiff and the Class, about the breach of security of Plaintiff's and the Class's Customer Data after Defendant knew or should have known that the data breach occurred.

147. Defendant's business practices, and each of them, are unfair because they offend established public policy and/or are immoral, unethical, oppressive, unscrupulous and/or substantially injurious to consumer in that Plaintiff and the Class suffered harm directly resulting from Defendant's failure to properly maintain Plaintiff's and the Class's Customer Data and failed to provide Plaintiff and the Class with timely and accurate notice. Plaintiff and the Class suffered the damages alleged above as a direct result of Defendant's failure to properly maintain Plaintiff's and the Class's Customer Data and its delay in providing timely and accurate notice of the Data Breach. This failure constitutes a violation of the UCL.

148. Plaintiff and the Class are further injured when Defendant continues to operate without having a proper security protocol in place. Defendant failed to exercise reasonable care in implementing and maintaining reasonable procedures and practice appropriate for maintaining the safety and security of Plaintiff's and the Class's Customer Data in its possession, custody, and/or control. This failure constitutes a violation of the UCL.

149. Defendant's business practices are unlawful and violates California Civil Code §§ 1798.81.5 and 1798.82 as more fully set forth above.

150. Plaintiff and the Class are entitled to relief, to the greatest extent permitted by law, which may not have been obtained by Defendant as a result of such business acts or practices, and enjoining Defendant from engaging in the practices described herein in the future.

151. Plaintiffs are entitled to an award of attorney's fees and costs pursuant to, *inter alia,* California Code of Civil Procedure § 1021.5.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class members pray for judgment against Defendant as follows:

a. An Order certifying the proposed Class and appointing Plaintiff as Class representative and her undersigned counsel of record as Class counsel;

b. In the alternative, an Order certifying the proposed California Subclass and appointing Plaintiff as representative of the California Subclass and her undersigned counsel of record as counsel for the California Subclass;

c. All recoverable compensatory and other damages sustained by Plaintiff and the Class members;

d. An Order permanently enjoining Defendant from engaging in the unlawful practices, and requiring it to employ reasonable and industry standard data security practices, as alleged herein;

e. All other appropriate equitable relief, including restitution and disgorgement;

f. Statutory pre-judgment and post-judgment interest on any amounts;

g. Payment of reasonable attorneys' fees and costs; and

h. Such other and further relief as this Court may deem just and proper.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

JURY DEMAND

Plaintiff demands a trial by jury on all causes of action so triable.

DATED: December 6, 2018

PEARSON, SIMON & WARSHAW, LLP
DANIEL L. WARSHAW

By: */s/ Daniel L. Warshaw*
DANIEL L. WARSHAW

Daniel L. Warshaw (Bar No. 185365)
dwarshaw@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
15165 Ventura Boulevard, Suite 400
Sherman Oaks, CA 91403
Telephone: (818) 788-8300
Facsimile: (818) 788-8104

Melissa S. Weiner (Pro Hac Vice Forthcoming)
mweiner@pswlaw.com
Joseph C. Bourne (Bar No. 308196)
jbourne@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
800 LaSalle Avenue, Suite 2150
Minneapolis, Minnesota 55402
Telephone: (612) 389-0600
Facsimile: (612) 389-0610

Alexander L. Simon (Bar No. 305734)
asimon@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
44 Montgomery Street, Suite 2450
San Francisco, CA 94104
Telephone: (415) 433-9000
Facsimile: (415) 433-9008

Attorneys for Plaintiff Dianne King

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403